

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:

Wasilewski, et al.

Serial No.: 10/602,986

Filed: June 25, 2003

Confirmation No.: 3781

Group Art Unit: 2131

Examiner: Chai, Longbit

Docket No.: A-9233 (191930-1560)

For: Method for Partially Encrypting Program Data

AFFIDAVIT OF HOWARD PINDER

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

I, Howard Pinder, declare as follows:

Education and Experience

1. I am an employee of the assignee of the 10/602,986 application.
2. I received a Bachelor of Science degree from the Georgia Institute of Technology in June, 1984, and a Master of Science degree from the Georgia Institute of Technology in September, 1991.
3. I am an inventor or co-inventor on 17 U.S. patents.
4. I have worked for over 21 years in electrical engineering, and have contributed to the advancement of electrical engineering science and technology, specializing in broadcast security and conditional access and embedded systems design.

5. I, with others, designed the PowerKEY conditional access system, which has been deployed in over 20 million decoder devices, and is one of the two predominant conditional access technologies used in the North American cable television market.
6. I co-invented methods for reconfiguring decoder secure memory, a method for encrypting the payload of an MPEG-2 Transport packet, several separate aspects of conditional access technology and devices, and methods for controlling digital bitrates through devices using MPEG-2 transport.
7. I have spent the last 15 years designing products that use MPEG-2 Transport technology, including digital cable headend products such as audio encoders, QAM modulators, bulk encryptors, and multiplexers. In these products I have specialized in the portions of the design concerned with scrambling or encryption of MPEG-2 transport packets.
8. I have from time to time participated in several standards bodies such as CableLabs, ATSC, and ATIS IIF.

Representative Claim 1

9. Representative claim 1 recites "a method for providing an instance in a conditional access system, the method comprising the steps of: selecting for encryption a digital bit stream from a plurality of digital bit streams using an identifier; encrypting the selected digital bit stream according to a first level encryption method to provide an encrypted instance; combining the encrypted instance with the plurality of digital bit streams to provide a partially-encrypted bit stream; and transmitting the partially-encrypted bit stream."

Examiner's Rejection of Claim 1 under 35 U.S.C. § 112, First Paragraph.

10. The Examiner asserts that "'selecting for encryption based on an [sic] packet identifier' is not specifically supported by the original disclosures of the instant application and claim limitations," Office Action Mailed November 14, 2006, p. 2. (Emphasis in original.)

Selecting for Encryption Using an Identifier as Understood by a Person of Ordinary Skill in the

Art

11. I assert that a person of ordinary skill in the art of digital encryption would disagree with the Examiner's conclusion for at least the following reasons.
12. Provisional application 60/054,575 contains the following disclosure for the cited claim language:

Each transport packet 703 has a packet identifier or PID, and all of the packets 703 that are carrying information for a given subcategory will have the same PID. Thus in FIG. 7, the packets carrying video 1 all have PID (a) and the packets belonging to that subcategory are identified by 705 (a). Similarly, the packets carrying audio 1 all have PID (b) and the packets belonging to that category are identified by 705 (b). A subcategory of information can thus be identified by the PID of its packets. As shown at output packets 707, the output from MUX 704 is a sequence of individual packets from the various subcategories. Any part or all of MPEG-2 transport stream 701 may be encrypted. In the preferred embodiment, the sets of packets making up program 709 are encrypted according to the DES algorithm, with the control word as the key.

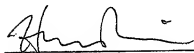
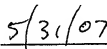
See Provisional Application 60/054,575, pg 28, lines 19-28.

13. A person of ordinary skill in the art would understand the cited passage from the provisional to disclose "selecting for encryption a digital bitstream from a plurality of digital bit streams using an identifier."
-
14. A person of ordinary skill in the art would understand the first four sentences of the paragraph to disclose the identification of packets using a PID (identifier).

15. A person of ordinary skill in the art would understand the output from MUX 704 is an MPEG-2 transport stream, referred to as MPEG-2 transport stream 701.
16. A person of ordinary skill in the art would understand the next two sentences of the paragraph to disclose that individual packets from the various subcategories may be encrypted, thereby disclosing a partially or fully encrypted bit stream.
17. A person of ordinary skill in the art would understand the next sentence of the paragraph to disclose an example of encrypting packets marked with PID 705(a) and 705(b), but not necessarily encrypting packets marked with some other PIDs.
18. A person of ordinary skill in the art would understand the seven sentences together, one following directly after the other, included in the same paragraph, to disclose "selecting for encryption a digital bitstream from a plurality of digital bit streams using an identifier."

DECLARATION

I hereby declare that all statements made herein are of my own knowledge are true and that all statements are made on information and belief and are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Howard Pinder****Date**